Ulyanikhin Evgeniy Ilyich
Student
Ural Federal University named after the first
President of Russia B.N. Yeltsin
Russia, Ekaterinburg
Academic supervisor: Kovaleva Alexandra Georgievna

BASIC METHODS OF MALWARE ANALYSIS BY DEEP NEURAL NETWORKS

Abstract. *This article discusses two methods for analyzing malicious attacks. The paper considers the consequences of insufficiently protected network devices and how algorithms of deep neural networks (DNN) cope with the task of eliminating malicious software.*

Keywords: *machine learning, information security, deep neural networks, DDOS attacks on Google, malware lifetime, image-processing technique.*

Ульянихин Евгений Ильич
Студент
Уральский Федеральный Университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ковалёва Александра Георгиевна

ОСНОВНЫЕ МЕТОДЫ АНАЛИЗА ВРЕДОНОСНЫХ ПРОГРАММ С ПОМОЩЬЮ ГЛУБОКИЙ НЕЙРОННЫХ СЕТЕЙ

Аннотация. *В этой статье рассмотрены два метода анализа вредоносных атак. Статья рассматривает последствия для недостаточно*

защищённых сетевых устройств и как алгоритмы глубокий нейронных сетей справляются с задачей устранения вредоносного программного обеспечения.

Ключевые слова: *машинное обучение, информационная безопасность, глубокие нейронные сети, DDOS-атаки на Google, время жизни вредоноса, техника image-processing.*

Everyone knows who actually writes malwares, but do everybody know what the average lifetime of a single malware is?

The malware attack is aimed at a large number of individuals or companies, and it is evident that someone sooner or later pays attention to a new trojan. The response time of antivirus software is approximately two hours, thus there is a fairly high probability that the malicious file will be destroyed in infected computers in two or three hours.

Unfortunately for users, the development of malware can be automated, and attackers can release malicious programs faster than updating antivirus databases.

The statistics of known DDoS attacks to Google network demonstrates the importance of the studied issues in the paper.

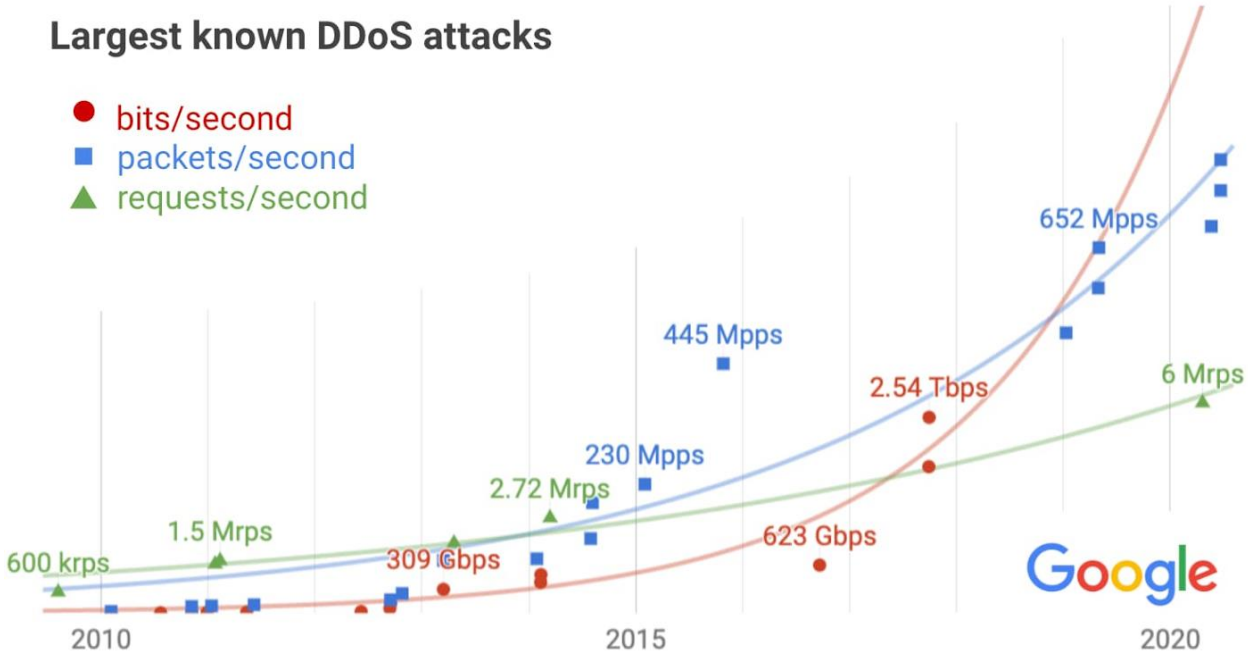

Figure 1 – Largest known DDoS attacks 0.

The exponential growth across all metrics is apparent, often generating alarmist headlines as attack volumes grow. But it is necessary to consider the exponential growth of the internet itself, which provides bandwidth and compute to defenders as well. After accounting the expected growth, the results are less concerning, though still problematic 0.

There are two methods for analyzing malware: static and dynamic. Static is a comparison of a suspect with signs of malware behavior. The comparison result confirms or not the status of suspected files. Dynamic is an analysis based on the file behavior: requests it makes, and actions it performs.

Malware attacks are in the rise, and nowadays new malware is easily generated as variants of existing malware thereby infecting more and more users' network devices. Therefore, it is important to study similar malware features that may help to classify them (malwares). Most malware variants are similar in structure, thus digital signal and image processing techniques may be used to classify malware.

Image processing: malware binaries were converted to black-white images demonstrating that the malware was similar in layout and texture, which indicates that the malware source is similar. Since image processing methods require neither design nor programming, they are compared to static and dynamic analysis. The main advantage of this approach is the ability to work with various malicious programs regardless of the operation system thus, covering the lion's share of network devices, including IoT.

Since this algorithm is proved to be quite effective, a dataset called MalImg was created based on numerous experiments, which is now used to evaluate the effectiveness of advanced machine learning algorithms 0.

Deep learning or Deep Neural Networks (DNNs) take inspiration from how the brain works and forms a sub module of artificial intelligence. The main strength of deep learning architectures is the capability to understand the meaning of data when it is in large amounts and to automatically tune the derived meaning with new data without the need for a domain expert knowledge.

Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are two types of deep learning architectures predominantly applied in real-life scenarios. Generally, CNN architectures are used for spatial data and RNN architectures are used for temporal data.

The concepts behind the various deep learning architectures are discussed in a mathematical way.

The explanation of how this happen (Figure) is obvious: there are not many people around the world who know computer literacy perfectly. Therefore, any unprepared interactions with the Internet increase the risk of infecting a network device and becoming a part of the botnet, which means becoming a part of the large-scale DDoS attack.

REFERENCES

1. Tarem Ahmed, Boris Oreshkin, Mark Coates. Machine learning approaches to network anomaly detection. – Text: electronic. – URL: https://www.researchgate.net/publication/234801644_Machine_learning_approaches_to_network_anomaly_detection (Reference date 16.10.2019). – 2007. – P. 16.

2. R. Vinayakumar, Mamoun Alazab, K. P. Soman, Prabaharan Poornachandran, Sitalakshmi Venkatraman. Robust Intelligent Malware Detection Using Deep Learning. – Text: electronic. – URL: https://ieeexplore.ieee.org/document/8681127 (Reference date 30.09.2020). – 2019. – P. 22.

3. Riaz Ullah Khan; Xiaosong Zhang; Mamoun Alazab; Rajesh Kumar. An Improved Convolutional Neural Network Model for Intrusion Detection in Networks. – Text: electronic. – URL: https://ieeexplore.ieee.org/document/8854549 (Reference date 15.11.2020). – 2019. – P. 4.

4. Chia-Mei Chen; Shi-Hao Wang; Dan-Wei Wen; Gu-Hsin Lai; Ming-Kung Sun. Applying Convolutional Neural Network for Malware Detection. – Text:

electronic. – URL: https://ieeexplore.ieee.org/document/8923568 (Reference date 15.11.2020). – 2019. P. – 5.

5. Exponential growth in DDoS attack volumes. – Text: electronic. – URL: https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks (Reference date 25.12.2020). – 2020.